Cloudflare WAF

實現現代應用程式安全性的 WAF

應用程式安全性挑戰

應用程式對企業的重要性一如既往，這就是為什麼攻擊者會持續不斷地針對它們，導致攻擊面擴大。

引起關注的問題包括：仍需防禦新興零時差漏洞利用、偵測規避嘗試、降低導致帳戶盜用的認證填充風險、偵測資料遺失，甚至搜尋上傳至應用程式的惡意程式碼。

除了上述問題，還必須確保應用程式保護是更廣泛的統一安全狀態的一部分，這種安全狀態也可保護 API、阻止機器人以及降低用戶端風險。而所有這一切必須在不會為團隊增添過度管理負擔的情況下進行。

Cloudflare WAF

Cloudflare Web 應用程式防火牆 (WAF) 是我們進階應用程式安全產品組合的基石，可確保應用程式安全且高效。只有 Cloudflare WAF 才能提供全面的安全可見性、提供針對 OWASP 攻擊和新興漏洞的分層保護、透過機器學習偵測規避和新攻擊、封鎖帳戶盜用、偵測資料遺失等，從而保護託管在任何地方的應用程式。我們強大的應用程式安全功能（例如 API 安全性和機器人緩解）與我們的 WAF 完全整合，呼叫同樣強大的規則引擎，由世界上第一款全球連通雲交付。

攻擊可見度和簡單上線

我們透過提供差異化的網路安全分析來視覺化所有流量，無論是否已緩解。對威脅狀況的即時可見性提供了明確的投資回報，讓團隊能夠瞭解他們的攻擊流量，以及在上線後應立即建立哪些保護。

針對新興攻擊的快速保護措施

由於每年都會出現數以萬計的漏洞，我們的 WAF 會快速新增新的受管規則，來封鎖對新發現的（零時差）漏洞的利用。我們的受管規則會封鎖漏洞利用，並輔以由機器學習衍生的 WAF 攻擊分數，以此偵測規避。

藉由龐大的全球網路獲取威脅情報

安全功效始於擁有最佳資料，我們龐大的全球網路代理了 20% 的網際網路，使我們能夠對威脅情勢擁有無與倫比的洞察力。這些資料為機器學習模型提供支援，我們可以將其與基於簽名的傳統偵測結合起來，以高精度發現並緩解攻擊嘗試。

 | + 886 8 0185 7030 | enterprise@cloudflare.com | www.cloudflare.com/zh-tw/

應用程式安全性挑戰

Cloudflare 提供更有效的保護。

我們透過分層保護提供更有效的 WAF 安全性：

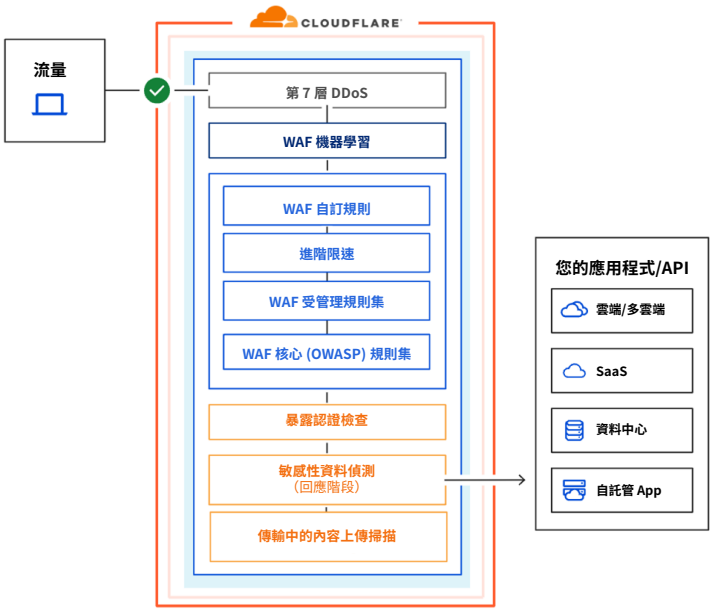
- 安全性分析
- 多個受管規則集
- 自訂規則
- 機器學習偵測
- 敏感性資料偵測
- 被盜認證檢查
- 進階限速
- 反惡意程式碼上傳掃描

Cloudflare 的回應速度更快。

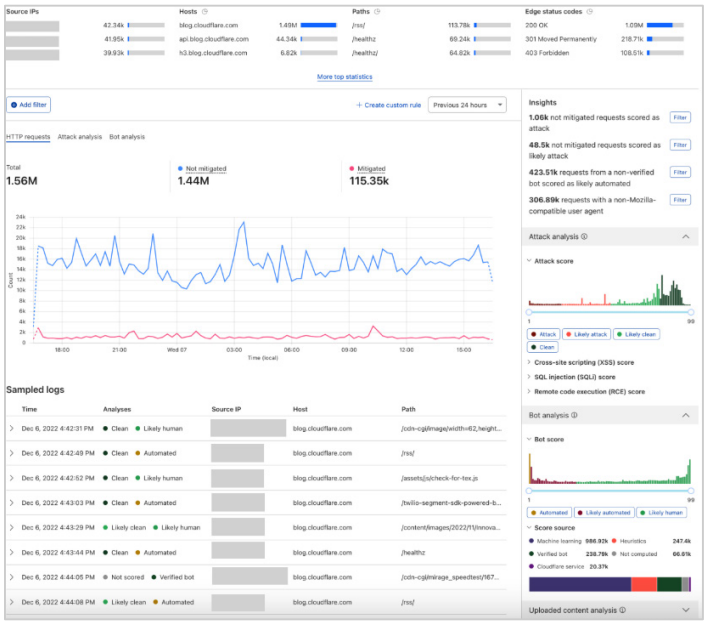
我們可以更快速地防禦漏洞利用。對於 HTTP/2 Rapid Reset、Log4j 和許多其他重大漏洞，我們部署了多個受管理規則，比其他 WAF 廠商快一個工作日。

Cloudflare 全面整合了應用程式安全性。

我們的 WAF 與其餘應用程式安全產品組合（包括 API Gateway 和 Bot Management）完全整合，全部透過 Cloudflare 的全球連通雲一次性交付。



WAF 安全性分析



實現企業級安全性的 WAF

SIEM 整合、SOC 就緒

經由 Cloudflare API 和原始記錄的整合，它可以輕鬆與您的 SIEM 整合，或透過 Cloudflare 提供的情報強化您的安全運營中心 (SOC)。

DevSecOps 讓一切更簡單

我們開箱即用的 Terraform 整合很自然地將應用程式安全性整合到 DevOps 做法中。

由 Cloudforce One 提供支援

Cloudflare 應用程式安全性從我們的威脅運作團隊 Cloudforce One 接收威脅情報，透過基於新興情報和 TTP 的全新偵測封鎖威脅。

Web 應用程式安全性	
多個 WAF 規則集的分層保護	使用多個規則集來阻止任何請求元件中的惡意負載： 1. Cloudflare 受管規則 2. OWASP 核心規則集 3. 用於阻止任何攻擊的自訂規則。 新的受管規則經過大流量測試，以確保最少的誤判。
更新零時差保護規則	Cloudflare 安全團隊不斷更新規則，在修補程式或更新可用之前防禦新的攻擊和零時差漏洞利用。
機器學習偵測	使用機器學習模型阻止繞過嘗試，為分層規則集提供補充。規則可以使用四種不同的攻擊分數：整體 WAF 攻擊分數、XSS 攻擊分數、SQLi 攻擊分數、RCE 攻擊分數。
針對主要 CMS 與電子商務平台的特定平台規則集	預設提供 WordPress、Joomla、Plone、Drupal、Magneto、IIS 等平台的保護，不需要額外收費。
自訂規則設定	部署規則或規則集時，使用以下動作來建立主動或被動安全性模型：BLOCK、MANAGED CHALLENGE、JS CHALLENGE、SKIP、LOG、LEGACY CAPTCHA、CUSTOM RESPONSES。
進階限速	阻止針對應用程式及 API 的濫用、DDoS 攻擊和暴力嘗試，方法是對個別 IP 限速或依標頭屬性（例如，金鑰、cookie、權杖）、ASN 或國家/地區進行限速。
敏感性資料偵測	偵測含有個人識別資訊、財務資訊、信用卡號或密碼（例如，API 金鑰）等敏感性資料的回應。
暴露認證檢查	在終端使用者帳戶被盜用之前，偵測使用被盜認證進行的認證填充攻擊。
內容上傳掃描	WAF Content Scanning 將掃描上傳的檔案以確定是否存在惡意程式碼，您可以透過建立自訂規則將其訊號與請求的其他參數結合起來。
SSL/TLS	為您的應用程式完全卸載和設定 SSL 流量。
更少的誤判	新規則經過大流量測試，以確保最少的誤判。
支援 gRPC 和 Websocket	gRPC 和 Websocket 端點的代理和安全流量。
可自訂的封鎖頁面	為訪客自訂包含適當詳細資訊的封鎖頁面。
與更廣泛的 Cloudflare 產品套件完整整合	改善應用程式效能、地理位置路由流量和利用邊緣運算。

可見度、報告和可程式性	
安全性分析	視覺化由機器學習評分的所有潛在攻擊。
即時記錄和原始記錄檔案的存取	取得可見度以幫助您微調 WAF；對所有 WAF 請求進行深入分析。
負載記錄	記錄並加密惡意負載以進行事件分析。
SIEM 整合	將記錄直接推送至現有的 SIEM 或從中提取記錄。
Terraform 整合	將應用程式安全性整合到 CI/CD 工作流程。
管理	
單一主控台管理	透過單一控制台簡化管理，來部署和管理全球應用程式的安全性和效能。
帳戶層級管理	透過針對所有網域進行單一帳戶層級的 WAF 設定，節省 WAF 管理的時間。
高可用性 — 採用 SLA	100% 正常運作時間保證，包括違反 SLA 時的補償金。
不需要硬體、軟體或調整	只需簡單變更 DNS 即可部署。
PCI 認證	Cloudflare 擁有 1 級服務提供者認證。
FedRAMP 已授權	我們的 Cloudflare for Government 套件（包括應用程式安全性）已獲得 FedRAMP 授權。

想要瞭解更多資訊？請註冊觀看我們的應用程式安全示範系列。

 | + 886 8 0185 7030 | enterprise@cloudflare.com | www.cloudflare.com/zh-tw/ REV:PMM-JAN-2025